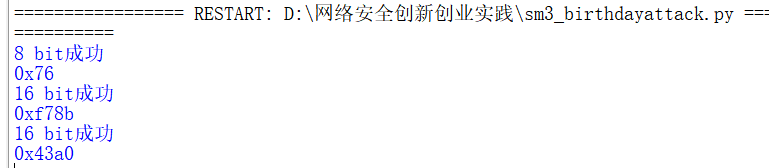
Project: implement the naïve birthday attack of reduced SM3



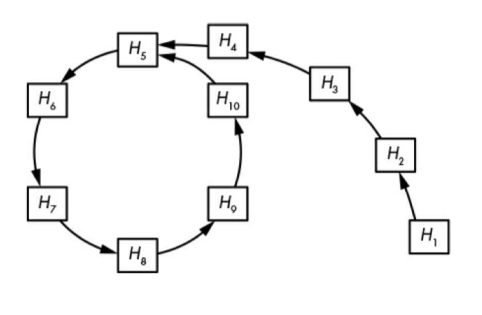
Project: implement the Rho method of reduced SM3

李晨漪

可直接运行

思路：

通过RHO算法，不断迭代，可能成环，寻找碰撞。



运行结果

当碰撞的bit数增大时，算法运行时间也增大。

